

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-094400
(43)Date of publication of application : 19.04.1991

105
Translate

(51)Int.Cl.

G07G 1/12

(21)Application number : 01-233708

(71)Applicant : NEC CORP

(22)Date of filing : 07.09.1989

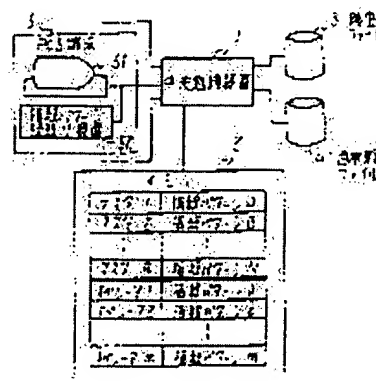
(72)Inventor : SUMIYA KENJI
SUNAGO MASAHIRO

(54) POS TERMINAL ACCESS SYSTEM

(57)Abstract:

PURPOSE: To prevent a secret file from being illegally destructed, updated and referred to by collating and inspecting the previously registered finger print patterns of a master and an operator with that obtained from a POS terminal and selectively applying the access right of the secret file and a normal operation file.

CONSTITUTION: A finger print pattern reader 52 optically reads out a finger print and forms a finger print pattern by impressing a finger to the reader. A CPU 1 inputs the finger print pattern based on a command outputted from the POS terminal 5 and collates and retrieves the entered pattern with the finger pattern in the memory 2. At the time of deciding that the entered pattern is not the master finger print, the CPU decides whether the pattern is the operator's finger print or not, and when the pattern is the operator's finger print, the access right is applied only to the normal operation file 4. If the pattern is not the operator's finger print, the CPU 1 applies a processing stop command to the POS terminal 5 to inhibit the succeeding processing. Consequently, the access right of the secret file in the POS system is not illegally provided.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑫ 公開特許公報(A)

平3-94400

⑤Int.Cl.⁵

G 07 G 1/12

識別記号

3 4 1 F

庁内整理番号

8610-3E

④公開 平成3年(1991)4月19日

審査請求 未請求 請求項の数 1 (全3頁)

⑭発明の名称 POS端末アクセス方式

⑯特 願 平1-233708

⑰出 願 平1(1989)9月7日

⑱発明者 角 谷 憲 二 東京都港区芝5丁目33番1号 日本電気株式会社内
⑲発明者 砂 子 昌 浩 東京都港区芝5丁目33番1号 日本電気株式会社内
⑳出願人 日本電気株式会社 東京都港区芝5丁目7番1号
㉑代理人 弁理士 内 原 晋

明 細 書

発明の名称

POS端末アクセス方式

特許請求の範囲

機密ファイルと通常業務ファイルとを有するPOSシステムにおいて、予め登録したマスクとオペレータとのそれぞれの指数パターンをPOSシステム本体のメモリに格納した指紋パターン記憶手段と、複数のPOS端末のそれぞれに設けられて光学的に指紋パターンを読取る指紋パターン読取り手段と、POS端末からの指紋パターンを前記指紋パターン記憶手段から照合・検査してマスクのものか、オペレータのものかを判定する指紋判定手段と、この指紋判定手段がマスクのものと判定したときは機密ファイルへアクセス権を与える処理手段とを有することを特徴とするPOS端末アクセス方式。

発明の詳細な説明

〔産業上の利用分野〕

本発明はPOS端末アクセス方式、特に機密ファイルおよび通常業務ファイルを有するPOS(POINT OF SALES)システムにアクセスするPOS端末アクセス方式に関する。

〔従来の技術〕

従来、この種のPOS端末アクセス方式は、POS端末がマスクキーおよびオペレータキーによって施錠されるようになっていて、マスクキーを使用すれば機密ファイルの変更および参照が可能となり、オペレータキーを使用した場合は機密ファイルの変更および参照ができず、通常業務ファイルのみにアクセスできるように構成されている。

〔発明が解決しようとする課題〕

上述した従来のPOS端末アクセス方式は、マスクキーとオペレータキーとの2種を利用して施錠されるようになっていて、マスクキーの保有者以外の人が何らかの方法でマスクキーを入手

し、使用した場合には、不正にPOSシステム内の機密ファイルのアクセス権を与えてしまう欠点がある。また、マスタキーおよびオペレータキーを紛失した場合には業務に停滯を生ずる欠点がある。

〔課題を解決するための手段〕

本発明のPOS端末アクセス方式は、機密ファイルと通常業務ファイルとを有するPOSシステムにおいて、予め登録したマスタとオペレータとのそれぞれの指数パターンをPOSシステム本体のメモリに格納した指紋パターン記憶手段と、複数のPOS端末のそれぞれに設けられて光学的に指紋パターンを読取る指紋パターン読取り手段と、POS端末からの指紋パターンを前記指紋パターン記憶手段から照合・検査してマスタのものか、オペレータのものかを判定する指紋判定手段と、この指紋判定手段がマスタのものと判定したときは機密ファイルへアクセス権を与える処理手段とを有することにより構成される。

〔実施例〕

検索する(ステップ②)。次いでマスタの指紋のものであるかを判定し(ステップ③)、マスタの指紋のものであれば機密ファイル3および通常業務ファイル4のアクセス権を与える(ステップ④)。ステップ③でマスタのものでなければオペレータの指紋であるかを判定し(ステップ⑤)、オペレータのものであれば通常業務ファイル4のみのアクセス権を与える。ステップ⑤でオペレータのものでなければ、POS端末5に処理停止の指示を与えて、以降の処理を行なわない(ステップ⑦)。

〔発明の効果〕

以上説明したように本発明は、予め登録したマスタおよびオペレータの指紋パターンとPOS端末から得られる指紋パターンとを照合・検査して、機密ファイルと通常業務ファイルとのアクセス権を選定して与えることにより、不正に機密ファイルや通常業務ファイルの破壊、更新、参照されることを防止でき、従来のキーによる場合のキーの紛失、キー持参忘れ等も無くすることができる効

次に、本発明の実施例について図面を参照して説明する。

第1図は本発明の一実施例の構成図で、POS本体を構成する中央処理装置1、中央処理装置1に接続され複数のマスタおよびオペレータのそれぞれの指紋パターンを格納しているメモリ2、および中央処理装置1に接続された機密ファイル3ならびに通常業務ファイル4と、表示付キーボード51および指紋パターン読取り装置52を有する複数のPOS端末5とを有する構成となっている。メモリ2に格納されている指紋パターンは、予め特定のPOS端末を用いて登録される。

第2図は第1図においてPOS端末5を操作するときの中央処理装置1のフロー図で、第2図を参照して第1図の動作の説明を進めると、先ず指紋パターン読取り装置52は指を押当てられることにより、光学的に指紋を読取り指紋パターンを作成する。POS端末5からのコマンドにより中央処理装置1はこの指紋パターンを取込んで(ステップ①)、メモリ2内の指紋パターンと照合・

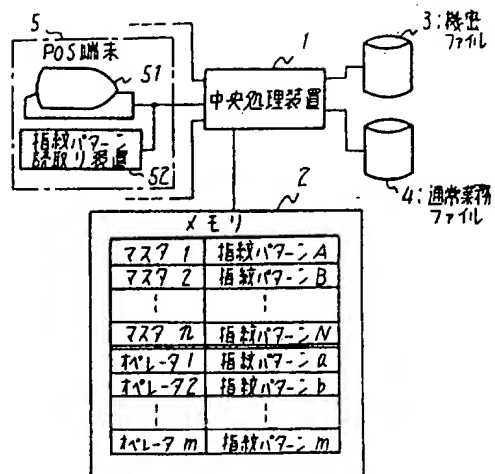
果がある。

図面の簡単な説明

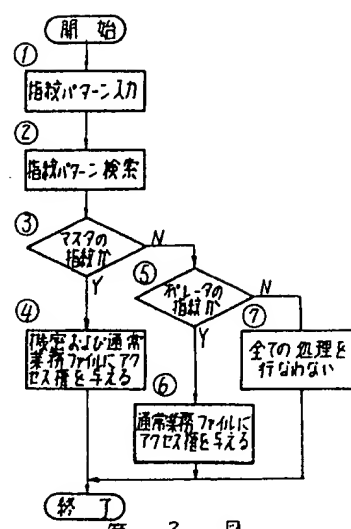
第1図は本発明の一実施例の構成図、第2図は第1図の動作のフロー図である。

1…中央処理装置、2…メモリ、3…機密ファイル、4…通常業務ファイル、5…POS端末、52…指紋パターン読取り装置。

代理人 弁理士 内 原 晋



第 1 図



第 2 図